

REMARKS

The Office Action dated August 24, 2006, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-32 are currently pending in the application, of which claims 1, 8, 15, 17, 24, and 31 are independent claims. Claims 1-30 have been amended, and claims 31-32 have been added, to more particularly point out and distinctly claim the invention. No new matter has been added. Claims 1-32 are respectfully submitted for consideration.

Claims 1, 5-6, 8, 12-13, 15, 17, 21-22, 24, and 28-29 were rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2003/0065685 of Belcaid et al. ("Belcaid"). Applicants respectfully traverse this rejection.

Claim 1, upon which claims 2-7 depend, is directed to a method including receiving a second data record to be stored on a database. The method also includes retrieving a first integrity checksum stored with a first data record previous to the second data record. The method further includes computing a second integrity checksum for the second data record with a cryptographic method based on a storage key, the retrieved first integrity checksum and the second data record. The method additionally includes storing the second data record and the second integrity checksum on the database.

Claim 8, upon which claims 9-14 depend, is directed to a method including retrieving a second data record to be verified from a first database. The method also

includes retrieving a second integrity checksum of the second data record. The method further includes retrieving a first integrity checksum of a first data record previous to the retrieved second data record. The method additionally includes computing a third integrity checksum for the second data record based on the retrieved second data record, the first integrity checksum, and a storage key. The method also includes comparing the second integrity checksum to the third integrity checksum, wherein the second data record is considered authentic when the second integrity checksum and the third integrity checksums are equal.

Claim 15, upon which claim 16 depends, is directed to a system including a database configured to store and provide signed data. The system also includes a data source configured to provide data records to be stored on the database system. The system further includes a signing entity configured to sign data records to be stored on the database system with a second integrity checksum computed based on a second data record, a first integrity checksum of the first data record previous to the second data record to be signed, and a storage key. The system additionally includes a verification entity configured to verify integrity of chosen data records by computing a computed third integrity checksum based on the second data record, the first integrity checksum of the first data record previous to the second data record, and the storage key, and comparing the computed third integrity checksum to the second integrity checksum stored on the database.

Claim 17, upon which claims 18-23 depend, is directed to a computer program embodied on a computer readable medium, said computer program for storing data records on a database system in which a signing entity is used for signing data records, wherein the computer program performs a process when executed in a computer device. The process includes receiving a second data record to be stored on a database. The process also includes retrieving a first integrity checksum stored with a first data record previous to the second data record. The process further includes computing a second integrity checksum for the second data record with a cryptographic method based on a storage key, the retrieved first integrity checksum and the second data record. The process additionally includes storing the second data record and the second integrity checksum on the database.

Claim 24, upon which claims 25-30 depend is directed to a computer program embodied a computer-readable medium for verifying the integrity of data records on a database, wherein the computer program performs a process when executed in a computer device. The process includes retrieving a second data record to be verified from a database. The process also includes retrieving a second integrity checksum of the second data record to be verified from a database. The process further includes retrieving a first integrity checksum of a first data record previous to the retrieved second data record. The process additionally includes computing a third integrity checksum for the second data record based on the retrieved second data record, the first integrity checksum, and a storage key. The process also includes comparing the second integrity

checksum to the third integrity checksum, wherein the second data record is considered authentic when the second integrity checksum and the third integrity checksums are equal.

Applicants respectfully submit that Belcaid fails to disclose or suggest all of the elements of any of the presently pending claims.

Belcaid generally relates to data recovery in a distributed system. Certain embodiments of Belcaid can, for example, provide an advantage that only the data elements that differ are updated, and thus no data is transmitted in vain and the network load is minimized.

In Belcaid, a distributed system maintains data in at least two databases. The data includes at least one data element. The amount of data transmitted during data recovery is minimized by comparing (210) a first total of the data element of the data in a first database with a second total of a corresponding data element of corresponding data in a second database. An updating procedure for the data element is initiated (213, 214) if the first total and second total are not the same.

Claim 1 recites “retrieving a first integrity checksum stored with a first data record previous to the second data record” and “computing a second integrity checksum for the second data record with a cryptographic method based on a storage key, the retrieved first integrity checksum and the second data record.” Applicants respectfully submit that these features are not disclosed by Belcaid.

The Office Action took the position that these features are disclosed by Belcaid at paragraph [0025]. The Office Action took the position that the “retrieving” feature is disclosed by Belcaid’s receiving, by the slave database, the checksum C of data A from the master database. The Office Action took the position that the “computing” feature is disclosed by Belcaid’s calculating, by the slave database, a checksum C’ for the corresponding data A’.

Applicants respectfully note that data A and data A’ (nor their corresponding checksums C and C’) are not related as recited in the claims. Claim 1, for example, recites “a second data record” and “a first data record previous to the second data record.” Data A and data A’ (nor their corresponding checksums C and C’) are not related as one being previous to the other. The two are not even in the same database. In fact, they are corresponding data in a corresponding database. Accordingly, data A of Belcaid cannot correspond to the claimed “first data record previous to the second data record” because Belcaid does not disclose an ordinal relationship between data A and data A’, but rather a parallel relationship, using the word “corresponding.”

Furthermore, in Belcaid, the slave database retrieves corresponding data A’ from its memory, as the Office Action admitted at page 2, item 6. Accordingly, corresponding data A’ is not “to be stored” (as recited by claim 1) but is already stored. Therefore, Belcaid cannot disclose or suggest “retrieving a first integrity checksum stored with a first data record previous to the second data record” as recited by claim 1.

Likewise, Belcaid indicates that checksum C and checksum C' are computed in "using the same rules," at paragraph [0025]. Paragraph [0024] explains that checksum C is calculated either from the data parts in data A or from the information parts in data A. Accordingly, neither checksum C nor checksum C' is computed "based on a storage key, the retrieved first integrity checksum and the second data record" as recited by claim 1. Instead, the checksums in Belcaid are calculated based only on data A (either its information parts or its data parts) or only on data A' (either its information parts or its data parts). Therefore, Belcaid cannot disclose or suggest "computing a second integrity checksum for the second data record with a cryptographic method based on a storage key, the retrieved first integrity checksum and the second data record" as recited by claim 1.

Additionally, claim 1 recites "storing the second data record and the second integrity checksum on the database." Applicants respectfully submit that this feature is also not disclosed or suggested by Belcaid.

The Office Action took the position that this feature is disclosed by Belcaid at paragraph [0032]. However, the cited paragraph indicates only that "the master database starts to update the indicated data elements to the slave database." In Belcaid, the checksum C is not part of the data elements, but is calculated therefrom. Furthermore, Belcaid requires the slave database to calculate its own checksum C' of the stored data, precisely because it cannot simply retrieve such a stored checksum. Accordingly, Applicants respectfully submit that Belcaid cannot disclose or suggest "storing the

second data record and the second integrity checksum on the database” as recited by claim 1.

Therefore, because Belcaid fails to disclose at least the features “retrieving a first integrity checksum stored with a first data record previous to the second data record,” “computing a second integrity checksum for the second data record with a cryptographic method based on a storage key, the retrieved first integrity checksum and the second data record,” and “storing the second data record and the second integrity checksum on the database” it is respectfully requested that the rejection of claim 1 be withdrawn.

Claim 8, 15, 17, and 24 each have their own individual scope, but recite several similar limitations, as identified below:

- “retrieving a second integrity checksum of the second data record,” “retrieving a first integrity checksum of a first data record previous to the retrieved second data record,” and “computing a third integrity checksum for the second data record based on the retrieved second data record, the first integrity checksum, and a storage key” (claim 8)
- “a signing entity configured to sign data records to be stored on the database system with a second integrity checksum computed based on a second data record, a first integrity checksum of the first data record previous to the second data record to be signed, and a storage key” and “a verification entity configured to verify integrity of chosen data records by computing a computed third integrity checksum based on the second data

record, the first integrity checksum of the first data record previous to the second data record, and the storage key, and comparing the computed third integrity checksum to the second integrity checksum stored on the database” (claim 15)

- “retrieving a first integrity checksum stored with a first data record previous to the second data record,” “computing a second integrity checksum for the second data record with a cryptographic method based on a storage key, the retrieved first integrity checksum and the second data record,” and “storing the second data record and the second integrity checksum on the database” (claim 17)
- “retrieving a second integrity checksum of the second data record to be verified from a database,” “retrieving a first integrity checksum of a first data record previous to the retrieved second data record,” and “computing a third integrity checksum for the second data record based on the retrieved second data record, the first integrity checksum, and a storage key” (claim 24)

Applicants respectfully submit that Belcaid also fails to disclose or suggest the above-identified features of claims 8, 15, 17, and 24.

The Office Action generally relied on the same teachings of Belcaid to disclose the above-identified features of claims 8, 15, 17, and 24. However, the Office Action additionally cited paragraph [0027] of Belcaid.

Paragraph [0027] of Belcaid does not rescue the Office Action's position. In paragraph [0027], Belcaid's slave database retrieves CS' from its own database, and then compares CS' to a retrieved CS from the master database. CS is an information part of data A, in Belcaid.

Accordingly, Belcaid is unable to disclose or suggest the above-identified features of claims 8, 15, 17, and 24, because the cited paragraph does not modify the relationship between Belcaid's master database and Belcaid's slave database from "corresponding" to "previous to" (as recited by each of claims 8, 15, 17, and 24) and because it does not disclose or suggest a different computation scheme than set forth in paragraphs [0024] of Belcaid. It is, therefore, respectfully submitted that Belcaid fails to disclose or suggest all of the elements of claims 8, 15, 17, and 24, and it is respectfully requested that the rejections of claims 8, 15, 17, and 24.

Furthermore, claims 8 and 24 specifically recite that a record is "considered authentic" under certain conditions. Belcaid does not disclose or suggest any such authentication procedure. Belcaid is concerned with data recovery, not authentication. Accordingly, Belcaid does not address whether any record is "considered authentic." Instead Belcaid is concerned with identifying whether the data in the slave database is properly synchronized with the data in the master database. Accordingly, it is respectfully submitted that Belcaid fails to disclose or suggest these further recitations of claims 8 and 24.

Applicants also call to the Examiner's attention to the way in which "previous to" (as recited in the claims) is described in the present specification. As can be seen, for example, in paragraph [0024] of the present application, the term "previous to" is used in an intra-database context. Thus, paragraph [0024] cautions that "If the integrity checksum is always read from a database, a malicious database administrator may delete the last row of the database without problems, as the chain of the integrity checksums will not break." Applicants note that the claim limitations must be read in light of the specification without reading limitations from the specification into the claims.

Thus, the present specification describes, for example, a method for securing the integrity of a database. The integrity can be secured by computing an integrity checksum for each data record. The checksum of the previous data record can be used in the computation.

A properly illuminated understanding of the terms of the claims, highlights yet another distinction between claims 1, 8, 15, 17, and 24 and Belcaid. Belcaid fails to disclose or suggest an "integrity checksum" for each data record. Belcaid is not interested in the integrity but rather the consistency of the data records. Accordingly, Belcaid has not motivation to produce an integrity checksum, although Belcaid makes use of other kinds of checksums, as discussed above.

Indeed, because Belcaid is not directed to a system or method involving integrity checksums, but rather to consistency checking between databases, Belcaid requires the presence of at least two databases, whereas the present claims do not contain any such

limitation. Indeed, at least some embodiments of the present invention can exist with respect to a single database and even to one table within that database.

In Belcaid, the checksums are not integrity checksums, but rather are consistency checksums that are used to ensure that the same records in parallel databases are properly synchronized. In Belcaid, if the checksums are the same, it is understood that the underlying data is the same, and thus that slave database does not need to be updated as to that particular data record. Accordingly, it is respectfully submitted that Belcaid fails to disclose or suggest an “integrity checksum” as recited in claims 1, 8, 15, 17, and 24. It is, therefore, respectfully requested that the rejection of claims 1, 8, 15, 17, and 24 be withdrawn.

Claims 5-6, 12-13, 21-22, and 28-29 depend respectively from, and further limit, claims 1, 8, 17, and 24. It is, therefore, respectfully submitted that each of claims 5-6, 12-13, 21-22, and 28-29 recites subject matter that is neither disclosed nor suggested in Belcaid, and it is respectfully requested that the rejection of claims 5-6, 12-13, 21-22, and 28-29 be withdrawn.

Claims 2, 9, 16, 18, and 25 were rejected under 35 U.S.C. 103(a) as being unpatentable over Belcaid in view of U.S. Patent Application Publication No. 2003/0023850 of Brown et al. (“Brown”). The Office Action took the position that Belcaid discloses all of the features of the claims except those relating to public key infrastructure. The Office Action cited Brown to remedy the deficiencies of Belcaid. Applicants respectfully traverse this rejection.

Claims 2, 9, 16, 18, and 25 depend respectively from, and further limit, claims 1, 8, 15, 17, and 24. It is, thus, respectfully submitted that deficiencies of Belcaid noted above with regard to claims 1, 8, 15, 17, and 24 are also deficiencies of the combination of Belcaid and Brown as applied to claims 2, 9, 16, 18, and 25, because Brown does not remedy the above-identified deficiencies of Belcaid.

Brown generally relates to verifying messaging sessions by digital signature of participants. Accordingly, it is unsurprising that the various database-related features with regard to which Belcaid is deficient are not addressed in any way by Brown. Accordingly, it is respectfully submitted that Brown cannot remedy the deficiencies of Belcaid.

Furthermore, the combination of Belcaid and Brown would not have been obvious to one of ordinary skill in the art. Belcaid and Brown have radically different objectives. Belcaid aims to keep a master database and a slave database consistent. Brown aims to verify messaging sessions. These two fields of art are quite unrelated, and one of ordinary skill in the art of one would not have any reason to examine the teachings of the other. That they are in different areas of technology is evidenced by their differing classifications. Belcaid is classified in 707/200 and Brown is classified in 713/176.

Furthermore, there is no discussion in Belcaid that would suggest that a storage key is necessary to accomplish the computation of Belcaid's checksum. Accordingly, one of ordinary skill in the art would not have a basis upon which to search for other keys in other areas of art, such as the keys discussed in Brown.

Accordingly, it is respectfully submitted that combination constitutes improper hindsight reconstruction. The Office Action began with the template of claims 2, 9, 16, 18, and 25 and tried to reconstruct the invention within that template. To protect against such invalid and inappropriate hindsight reconstruction, the Federal Circuit has ruled that references cannot be selected, and selected elements from selected references cannot be combined, without some suggestion, motivation, or teaching that would render obvious that selection and that combination. *See, e.g., Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1385, 58 USPQ2d 1286, 1293 (Fed. Cir. 2001) (“In holding an invention obvious in view of a combination of references, there must be some suggestion, motivation, or teaching in the prior art that would have led a person of ordinary skill in the art to select the references and combine them in the way that would produce the claimed invention.”); and *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1124-25 (Fed. Cir. 2000) (“a showing of a suggestion, teaching, or motivation to combine the prior art references is an ‘essential component of an obviousness holding’”).

The proposed combination is deficient because there is no motivation to combine. The Office Action proposed that the motivation to combine would have been “so that the integrity of the signing entity may be verified.” However, Belcaid does not include a signing entity, much less one that is in need of verification. Accordingly, Applicants respectfully submit that the proposed motivation to combine is inapplicable to the actual

proposed combination. Accordingly, it is respectfully requested that this rejection be withdrawn.

Claims 3, 10, 19, and 26 were rejected under 35 U.S.C. 103(a) as being unpatentable over Belcaid in view of U.S. Patent No. 4,864,616 of Pond et al. ("Pond"). The Office Action took the position that Belcaid discloses all the features of the claims except "wherein the integrity checksum for a first row of a database is a generated initialization vector." The Office Action cited Pond to remedy this deficiency of Belcaid. Applicants respectfully traverse this rejection.

Claims 3, 10, 19, and 26 depend respectively from, and further limit, claims 1, 8, 17, and 24. It is, thus, respectfully submitted that deficiencies of Belcaid noted above with regard to claims 1, 8, 17, and 24 are also deficiencies of the combination of Belcaid and Pond as applied to claims 3, 10, 19, and 26, because Pond does not remedy the above-identified deficiencies of Belcaid.

Pond generally relates to cryptographic labeling of electronically stored data. The data Pond is interested in is not database entries, but files of data, as can be seen at column 4, lines 58-66. Accordingly, it is unsurprising that the various database-related features with regard to which Belcaid is deficient are not addressed in any way by Pond. Accordingly, it is respectfully submitted that Pond cannot remedy the deficiencies of Belcaid. Thus, it is respectfully requested that the rejection of claims 3, 10, 19, and 26 be withdrawn.

Furthermore it would not have been obvious to combine the teachings of Pond and Belcaid. As explained above, in order to prevent inappropriate hindsight reconstruction, the Federal Circuit requires there be motivation in the prior art to make the combination. This suggestion test requires the Office Action to explain why one of ordinary skill in the art would be motivated to combine the references.

The Office Action took the position that the combination would have been motivated by the possibility of using an initialization vector in the computation of a second integrity checksum, where there is no previous integrity checksum available. Applicants respectfully disagree.

Belcaid's system does not require the use of a previous integrity checksum in its calculation of its checksum C. Accordingly, one of ordinary skill in the art considering how to improve Belcaid would not care whether or not a previous integrity checksum was available, and would not turn to Pond to provide the necessary features. Accordingly, it is respectfully submitted that there is no motivation to make the proposed combination. Therefore, for this additional reason, it is respectfully requested that the rejection of claims 3, 10, 19, and 26 be withdrawn.

Claims 4, 11, 20, and 27 were rejected 35 U.S.C. 103(a) as being unpatentable over Belcaid in view of allegedly admitted prior art, contained in the specification of the present application. Applicants respectfully submit that this rejection contains legal error, inasmuch as the combination of Belcaid with the disclosure of the present application constitutes legally impermissible hindsight reconstruction, because there is no

motivation, teaching, or suggestion in the prior art to make the combination. The Office Action does not even attempt to provide motivation to combine, and it is well established that motivation to combine may not be gleaned from Applicants' disclosure. It is, therefore, respectfully requested that this rejection be withdrawn.

Claims 7, 14, 23, and 30 were rejected under 35 U.S.C. 103(a) as being unpatentable over Belcaid in view of U.S. Patent No. 6,557,044 of Cain ("Cain"). The Office Action took the position that Belcaid discloses all of the elements of the claims except "wherein the integrity checksums comprises a running sequence number." The Office Action cited Cain to remedy this deficiency of Belcaid. Applicants respectfully traverse this rejection.

Claims 7, 14, 23, and 30 depend respectively from, and further limit, claims 1, 8, 17, and 24. It is, thus, respectfully submitted that deficiencies of Belcaid noted above with regard to claims 7, 14, 23, and 30 are also deficiencies of the combination of Belcaid and Cain as applied to claims 3, 10, 19, and 26, because Cain does not remedy the above-identified deficiencies of Belcaid.

Cain generally relates to a method and apparatus for exchange of routing database information. In Cain, a routing database is maintained including checksums that are used to identify changes in routes. Accordingly, it is unsurprising that the various database-related features with regard to which Belcaid is deficient are not addressed in any way by Cain. Accordingly, it is respectfully submitted that Cain cannot remedy the deficiencies

of Belcaid. Thus, it is respectfully requested that the rejection of claims 7, 14, 23, and 30 be withdrawn.

Furthermore it would not have been obvious to combine the teachings of Cain and Belcaid. As explained above, in order to prevent inappropriate hindsight reconstruction, the Federal Circuit requires there be motivation in the prior art to make the combination. This suggestion test requires the Office Action to explain why one of ordinary skill in the art would be motivated to combine the references.

Applicants respectfully submit that this rejection contains legal error, inasmuch as the combination of Belcaid with the disclosure of the present application constitutes legally impermissible hindsight reconstruction, because there is no motivation, teaching, or suggestion in the prior art to make the combination. The Office Action does not even attempt to provide motivation to combine, and it is well established that motivation to combine may not be gleaned from Applicants' disclosure. It is, therefore, respectfully requested that this rejection be withdrawn.

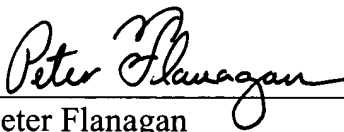
For the reasons explained above, it is respectfully submitted that each of claims 1-32 recites subject matter that is neither disclosed nor suggested in the cited art. It is, therefore, respectfully requested that all of claims 1-32 be allowed, and that this application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by

telephone, Applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Peter Flanagan
Registration No. 58,178

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

PCF:jkm:kh

Enclosures: Additional Claim Fee Transmittal
Check No. 15430